CVE-2014-1500

Keijo Lillo

Description

Mozilla Firefox before 28.0 and Mozilla SeaMonkey before 2.25 allow remote attackers to cause a denial of service (resource consumption and application hang) via *onbeforeunload* events that trigger background JavaScript execution.

When visiting URL of this bug and after loading the page the pop-up with the two buttons ("Stay" and "Leave") is shown.

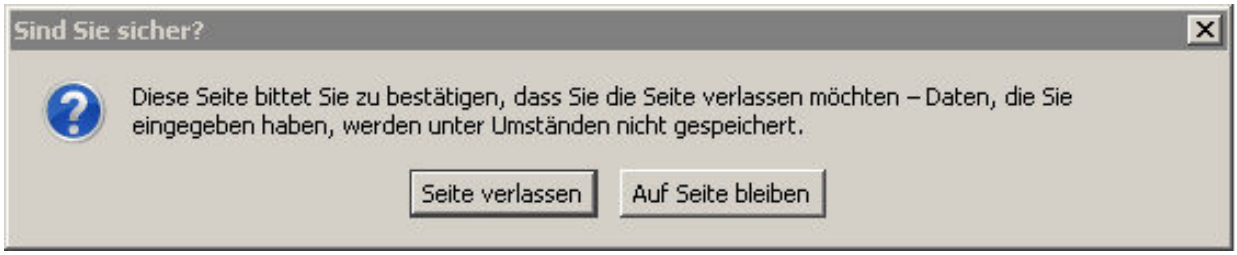

Figure 1. The button on the right hand side means „Stay" and the left button means „Leave".

For example, try to visit: http://tim-philipp-schaefers.de/poc/

As long as the user has not clicked on any of these buttons he can not close the tab, close the browser nor navigate in any other way in the browser: the browser has become unresponsive. This allows for a denial of service (DOS) attack due to resource consumption and blocks the ability of users to exit the application.
If the user clicks on "Leave", then these browsers all send a new *get*-request, to which server responds with a 304. If the user clicks on "stay" button, the browsers do not send any requests, but the dialog pops up immediately again. Hence it is an endless loop for the user.

User has only two options to get out of the endless loop:

1) close the tab when the page is reloading;

2) close the whole browser.

Solution

1) Change the navigation allowance section as it is shown on figures 2 and 3;

```
4149 nsDocShell::IsNavigationAllowed(bool aDisplayPrintErrorDialog)
4150 {
4151     return !IsPrintingOrPP(aDisplayPrintErrorDialog) && !mFiredUnloadEvent;
4152 }
```

Figure 2. Before changes.

```
4149 nsDocShell::IsNavigationAllowed(bool aDisplayPrintErrorDialog)
4150 {
4151   bool isAllowed = !IsPrintingOrPP(aDisplayPrintErrorDialog) && !mFiredUnloadEvent;
4152   if (!isAllowed) {
4153     return false;
4154   }
4155   if (!mContentViewer) {
4156     return true;
4157   }
4158   bool firingBeforeUnload;
4159   mContentViewer->GetBeforeUnloadFiring(&firingBeforeUnload);
4160   return !firingBeforeUnload;
4161 }
```

Figure 3. After changes.

2) Changes should be made also in nsDocumentViewer (Figure 4).

```
1237 NS_IMETHODIMP
1238 nsDocumentViewer::GetBeforeUnloadFiring(bool* aInEvent)
1239 {
1240   *aInEvent = mInPermitUnload;
1241   return NS_OK;
1242 }
1243
1244 NS_IMETHODIMP
1245 nsDocumentViewer::ResetCloseWindow()
```

Figure 4. Added code part

After these changes, if the „Stay“ button is pressed, the onload->reload flood will be stopped. Now it is possible to navigate in the browser and close the box by clicking on „Leave“ button or „x“ on upper right corner.

REFERENCES

1. Bugzilla@Mozilla. [WWW] https://bugzilla.mozilla.org/show_bug.cgi?id=956524 (30.05.2014)

2. CVE. [WWW] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1500 (30.05.2014)

3. Mozilla Foundation Security Advisory 2014-20. Mozilla. [WWW]

http://www.mozilla.org/security/announce/2014/mfsa2014-20.html (31.05.2014)

4. National Vulnerability Database. [WWW] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-1500 (31.05.2014)

5. Rapid7. [WWW] http://www.rapid7.com/db/vulnerabilities/mfsa2014-20-cve-2014-1500 (31.05.2014)